SECTION X. OPERATIONS SECURITY (OPSEC)

10-100 **Purpose.** This section provides information and instructions for uniform implementation of the DoD OPSEC program within the Defense Industrial Security Program.

10-101 General. The OPSEC program is a DoD directed effort, the mechanics of which are outlined in DoD Directive 5205.2 (DoD Operations Security Program, July 7, 1983).

a. The principal objective of OPSEC is to preclude the disclosure of classified information by-denying or reducing the opportunity of hostile intelligence services (HOIS) to gain access by directly observing/analyzing/evaluating our activities and operations, the awareness of which may lead to the compromise of classified information. Stated another way, OPSEC is the process of denying information about friendly intentions, capabilities plans, or programs by identifying, controlling, and protecting intelligence indicators associated with planning and conducting military operations as well as other defense activities.

b. Within the context of industrial security, the general aim of OPSEC is to promote mission effectiveness by preserving essential secrecy about U.S. intentions, capabilities, and current activities when the DISP procedures for safeguarding classified material and information require enhancement. Secrecy essential to defense activities may be compromised whenever open sources (such as technical articles, press “releases, National Technical Information Service publications, the Congressional Record, Commerce Business Daily, or contract awards) and detectable activities (such as communications, logistics actions, research, development and test activities, or radar emissions) provide information that can be pieced together or analyzed, to the detriment of U.S. interests. In some instances, such information or indicators are not addressed by DISP requirements for classified material and require in-depth analysis and case-by-case planning to identify them. The fundamental goal of the’ OPSEC process is to minimize or eliminate such indicators. OPSEC thus encompasses activities which are unique to the OPSEC process, i.e. , (a) determining, through threat/vulnerability analysis, whether there are unacceptable/ undesirable intelligence indicators and what they are; and (b) developing and implementing countermeasures to best eliminate or minimize them.

c. Contracts limited to classified information (such as those to process or evaluate information and produce classified documents, pictures, computer programs, training aids, and similar matters; for classified consultant, library, or ADP services; or for printing classified documents) generally do not require OPSEC. Contracts that involve system acquisition (such as those for weapon systems, Electronic Counteriueasures, radio transmitters, active sensors, or low observable capabilities) or sensitive activities (such as intelligence operations or testing foreign material) usually require OPSEC, particularly if such contracts involve special access. Contracts for such things as logistics support, personal or maintenance services, may or may not require OPSEC, depending on the situation.

d. OPSEC uses the same security measures that have been used to protect government information for years under the DISP but adds a new dimension. This new dimension or emphasis is the analysis, control and security of unclassified intelligence indicators. The object of this analysis and control is the protection of things we do, our operations, tests, and activities. As such, OPSEC is intended to complement the DISP.

e. The application of OPSEC measures supports the delicate balance between the need for secrecy, and the need to accomplish potentially detectable essential actions. This balance is threatened by the pervasive nature of the multidisciplined foreign intelligence activities directed against the U.S. The OPSEC process requires recognition of the intelligence threat, incorporation of OPSEC considerations into all stages of planning, and the application of appropriate protective measures. Effective OPSEC provides the best assurance that essential secrecy and surprise can be retained while denying the adversary an opportunity to develop effective countermeasures.

10-102 Application. The DoD OPSEC program is applicable only to Defense contractors participating in the DISP when the contracting User Agency determines that additional OPSEC measures are essential to protect classified information-for specific classified contracts and imposes OPSEC as a contractual requirement. OPSEC is concerned with all sources of exploitable information. The DISP generally covers only the classified information disclosure problem, while OPSEC covers the total problem by addressing vulnerabilities and countermeasures for a specific program. OPSEC is principally oriented to those instances in which evaluations indicate program weaknesses which could lead co the disclosure of classified information.

a. OPSEC will be directed to the protection of unclassified intelligence indicators on classified programs of such nature that the disclosure of the indicators may lead to the compromise of classified information. OPSEC is not intended as a vehicle to protect unclassified technology; other programs exist to protect this information (DoD 5230.25).

b . Requirements for OPSEC shall be included in the appropriate requisition documentation and resultant contract or addendum thereto in sufficient detail to ensure complete contractor understanding of exactly what special OPSEC provisions are required by the UA. Full disclosure of these requirements is essential so that" contractors can comply and charge attendant costs to the specific contracts for which they have been ordered. In providing such requirements, UA'S shall not solely refer to their internal regulations when imposing OPSEC requirements, but shall fully specify the particulars in the contract proper, and shall provide full information necessary to explain internal regulations. Additionally, applicable DD 254s shall be annotated to indicate that OPSEC requirements are contained in the contract or addendum thereto.

c. Contractual OPSEC requirements shall be strictly limited to those sensitive projects which clearly justify extraordinary security measures beyond those embodied in the DISP as outlined in the ISM. If the ISM provides a countermeasure or safeguard for a particular identified vulnerability concern, the ISM will be allowed to address it and

redundant countermeasures will not be added as contractual OPSEC requirements (e.g. information, physical or personnel security). UAs shall make this determination prior to imposing OPSEC measures. Assistance in this area is available to UAS from CSO's. Further, OPSEC requirements shall be based on the most current UA hostile intelligence threat and vulnerability assessment available, keyed to specific contractor areas, processes, activities, or facilities involved in classified contract performance.

d. DIS shall have principal responsibility for inspecting contractor compliance with OPSEC requirements. DIS may, however, be accompanied by cognizant UA representatives if requested. Visits by representatives of DoD Components to DISP facilities for OPSEC purposes will be coordinated with the Cognizant (Cog) DIS Office of Industrial Security (as much lead time as possible should be allowed). A representative of the Cog office may accompany the component member on the visit to the contractor; however, depending on the nature of visit, it will not always be necessary for the Cog office representative to be present. UA changes in OPSEC plans or requirements as a result of UA visits or evaluations will be provided to the Cog office.

e. DIS OPSEC inspections of contractors performing on classified contracts aboard military installations shall be performed only when requested by installation commanders.

10-103 Responsibilities.

a. UA procuring activities shall:

(1) If determined necessary to impose OPSEC measures, ensure that specific, detailed requirements for OPSEC are incorporated into any solicitation, and any resulting contract, subcontract, or addendum thereto so that the contractor will have a complete understanding of exactly what special security requirements in excess of ISM procedures are required by the User Agency". Full disclosure of these requirements is essential so that the contractor can comply with the -contract provisions. DD Forms 254 shall not be used for this purpose; however, they shall indicate that OPSEC.requirements are provided for in the applicable contracts.

(2) Provide the CSO full and detailed particulars of OPSEC requirements/measures and the DD 254s in each instance when such requirements are included in a classified contract awarded to industry. These include copies of the contract statement of work (SOW) when OPSEC requirements are included in such statement, UA approved OPSEC plans and requirements if contractually required, DD Form 1644, "Data Item Description, and DD Form 1423, "Contract Data Requirements List" (when these forms are used to convey OPSEC information or direct contractor submission of OPSEC documents/plans), etc. This information is needed to enable the CSO to inspect for compliance with OPSEC requirements during regularly scheduled DISP inspections.

(3). To the extent f easible, accompany and provide assistance * when requested, to the CSO during regularly scheduled security inspections * for assessment of compliance with contractually incorporated OPSEC measures. *

b. CSO shall: *

.(1) Designate an OPSEC Coordinator who will be the point of * contact for OPSEC matters within the Region. *

(2) Inspect contractor facilities when OPSEC requirements * have been contractually Incorporated into classified contracts to assess * contractor compliance with the OPSEC requirements. These shall be * accomplished: a) as part of a regularly scheduled industrial security * inspection, b) as part of an unannounced industrial security inspection. *

(3) Request the UA Contracting Officer to provide assis- * t ante in the conduct of OPSEC Inspections when deemed appropriate. *

(4) Coordinate visits by representatives of UA Contracting * Off icers to DISP facilities for OPSEC purposes. Every effort will be made * to cooperate with the component in accommodating the visit. *

10-104. Procedures for Inspecting OPSEC Programs. *

a. CSOs will use the approved OPSEC Plan/Requirements provided * them by the UA Contracting Officer as the basis for OPSEC inspections. *

b. When appropriate, the CSO will request a representative of * the UA Contracting Officer to accompany IS Reps during inspections of * industry OPSEC programs. *

c. Deficiencies of OPSEC contract requirements identified * during joint DIS/contracting office visits will be discussed between the * IS Rep and the contracting office representative before the briefing to * management and prior to citing the contractor for noncompliance. *

d. Def iciencies requiring remedial action identified during * the inspection of a contractor's OPSEC program will be included in the LOR * issued to the facility. Specific contract OPSEC requirements will be cited * as the basis for identified deficiencies. *

e. Satisfactory OPSEC inspection results shall not be routinely * distributed to UAs or the contracting offices having procurement responsi- * bilities at the inspected facilities. However, when remedial act ion is * required, the CSO shall furnish a copy of the inspection report to the UA * concerned. *